AFFIDAVIT OF NICOLE SORRELL IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Nicole Sorrell, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), and am assigned to the office of the Special Agent in Charge, Boston, Massachusetts. I have been an HSI agent since 2009. As part of my duties, I am authorized to investigate violations of United States law, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including but not limited to violations of 18 U.S.C. §§ 2422, 2423, 2251, and 2252A. I have received training in the investigation of child exploitation offenses, including child pornography, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).

2. I am currently participating in an investigation relating to violations of federal law by an individual utilizing Kik[1] usernames gayinvaderzim[2], kidzklub, and smudgedgraphite.

[1] Kik Messenger (hereinafter, "Kik") is a free instant messaging application for mobile devices used to transmit messages, images, videos, and other content.

[2] For ease of reference, I will hereinafter refer to the individual simply by the usernames gayinvaderzim, kidzklub, and smudgedgraphite.

3. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure to search the residence located at 74 Lancaster Road, Arlington, Massachusetts 02476 (the "SUBJECT PREMISES"), as more fully described in Attachment A, which is included herein by reference.

4. As described herein, there is probable cause to believe that the SUBJECT PREMISES contains contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A, which items are more specifically described in Attachment B, which is also incorporated herein by reference.

5. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of As described herein, there is probable cause to believe that the SUBJECT PREMISES contains contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A, which items are more specifically described in Attachment B, which is also incorporated herein by reference.

BACKGROUND ON KIK AND KIK REPORTS

6. Kik Messenger (hereinafter "Kik") is a mobile application designed for chatting or messaging. It was previously owned and operated by Kik Interactive, Inc., a Canadian company, but was acquired in October 2019 by a company based in the United States.[3] According to the publicly available document "Kik's Guide for Law Enforcement,"[4] to use this application, a user must download the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user creates an account, the user is able to locate other users via a search feature. While messaging, users are able to send each other text messages, images, and videos.

7. According to "Kik's Guide for Law Enforcement," Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text

---

[3] The information outlined in this affidavit regarding the suspect user was obtained from Kik before the company's American acquisition. The application's functionality remains substantially the same. As such, this affidavit references certain processes, features, etc., in the present tense, and specifically identifies reliance on documentation, guides, and policies that were in effect prior to the acquisition.

[4] Available at the writing of this affidavit at: https://help.kik.com/hc/en-us/articles/217681728-guide-for-Law-Enforcement.

messages, images and videos. These groups are administered by the group creator, who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or with any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

8. According to information provided to HSI by a Kik Law Enforcement Response Team Lead prior to the company's acquisition, Kik's Terms of Service prohibited Kik users from uploading, posting, sending, commenting on, or storing content that contains child pornography and/or child abuse images. The Terms of Service also provided that Kik may review, screen, and delete user content at any time, and may ban the user account, if Kik believes use of their services is in violation of the law. According to Kik, Kik had a strong business interest in enforcing their Terms of Service and ensuring that their services are free of illegal content, and in particular, child sexual abuse material. Accordingly, Kik reported that it independently and voluntarily took steps to monitor and safeguard their platform and that ridding Kik products and services of child abuse images was critically important to protecting their users, product, brand, and business interests.

9. Prior to October 2019 Kik was located in Ontario, Canada and governed by Canadian law. According to information contained in the available "Kik Interactive, Inc. Child Sexual Abuse and Illegal Material Report and Glossary" (hereinafter Kik Glossary), which Kik provided, when reporting information to law enforcement authorities, Kik was mandated to report to the

Royal Canadian Mounted Police (RCMP) any images and/or videos that would constitute suspected child pornography under Canadian law that were discovered on the Kik platform. According to the Kik Glossary, Kik was typically alerted to suspected child pornography on Kik based on digital hash value matches to previously identified child pornography, or through reports from other Kik users or third-party moderators. The RCMP has advised HSI agents that upon receiving a report from Kik related to suspected child pornography, the RCMP would review the reported IP addresse(s) of the Kik users contained in the Kik Reports to determine their location. The RCMP would then provide Kik Reports of Kik users in the United States to HSI in Ottawa, Canada, who in turn provided the Kik Reports to the HSI Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) located in Fairfax, Virginia for analysis and dissemination.

STATEMENT OF PROBABLE CAUSE

KIK REPORT 1

10. I have reviewed a Kik Report dated September 19, 2018. A review of the report shows that, on September 19, 2018, at 12:26:27.0 UTC, from IP[5] address 24.61.82.255, Kik user

[5] An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP

gayinvaderzim, who also provided the name Jail-Bait Zim, email address thatirkenscum@gmail.com, birthdate xx/xx/1995, and device type Samsung Android, used Kik to send an image depicting child pornography via the Kik platform. This image was detected by SafePhoto[6], a technology utilized by Kik to detect images of known child pornography.

11. A query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address/es 24.61.82.255 used on September 19, 2018 at 12:26:27.0 UTC to send a child pornography image was registered to Comcast Communications ("Comcast").

12. On January 28, 2019, HSI Boston issued a summons to Comcast regarding the IP address for the specific date and time as described in Paragraph 10. A review of the results obtained on

---

addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

[6] According to the Kik Glossary, Kik has developed an internal hash matching system called "SafePhoto" (similar to Microsoft's PhotoDNA system) that Kik uses to scan images uploaded via Kik for suspected child pornography. Kik's SafePhoto database is comprised of hash values obtained from the International Criminal Police Organization (hereinafter "INTERPOL"), the RCMP and the National Center for Missing and Exploited Children (hereinafter "NCMEC"). Kik uses SafePhoto to run a hash value check against every image sent within Kik, including within private conversations, in order to detect images that may depict suspected child pornography and prevent such images from continuing to circulate through their application. When a user sends an image with a hash value that matches a child exploitation hash value in the SafePhoto database, Kik removes the content from its communications system, closes the user's account and provides a SafePhoto report of the incident to the RCMP.

January 29, 2019, identified the following account holder and address, which is the address of the SUBJECT PREMISES: Jim Lister, 74 Lancaster Road, Arlington, Massachusetts, 02476.

13. A query of the Massachusetts Criminal Justice Information Service (CJIS) revealed the SUBJECT PREMISES to be the address on file for Mason LISTER, a registered Level 1 Sex Offender in the State of Massachusetts[7].

14. In October 2019, HSI Boston agents contacted the Arlington Police Department (APD). APD Detective James Smith informed HSI agents that LISTER was known to the APD. Detective Smith confirmed LISTER's current address to be the SUBJECT PREMISES. Detective Smith also confirmed the SUBJECT PREMISES to be the residence of James and Maureen Lister, who are Mason LISTER's parents. HSI Boston referred Kik Lead 1 to the Arlington Police Department for further investigation.

[7] The Sex Offender Registry Board (SORB) of Massachusetts requires convicted Sex Offenders to register with the SORB and provide current residential and employment addresses. The SORB classifies Sex Offenders based on their risk of re-offense and the degree of danger they pose. Information about the SORB is publicly available at: https://www.mass.gov/orgs/sex-offender-registry-board

KIK REPORT 2

15. I have reviewed a Kik report dated April 18, 2019. A review of the Kik Report shows that on April 18, 2019, an individual utilizing Kik username kidzklub, who provided the name Kids Club[8], email address unclejacknsfw@gmail.com, birthdate xx/xx/1999, and phone brand and model Samsung SM-T580, used Kik to send an image of child pornography, as described herein.

16. According to Kik's SafePhoto report, the reported image was flagged based upon a hash value provided to Kik by Interpol. According to information provided to HSI by INTERPOL[9], hash values[10] provided by INTERPOL to Kik are from the INTERPOL Baseline Hash (also known as IBH), a system that empowers third parties (both public and private networks) to recognize, report and remove known child (sexual) abuse material (CAM) by allowing them to check images and videos coming onto their networks, or already on their networks, against a

---

[8] This user also previously provided the names "Alex", "Gonzales", "Monloicth", and "Klub".

[9] INTERPOL, also known as the International Criminal Police Organization, is an inter-government organization which enables police in its' 194- member organization to work together to investigate international crime. INTERPOL provides investigative support, expertise, and training to law enforcement worldwide, focusing on three major areas of transnational crime: terrorism, cybercrime and international crime.

[10] I know from training and experience that a hash value is akin to a fingerprint for a digital file. In order to generate a hash value, the contents of a file are processed through a cryptographic algorithm, and a unique numerical value – the hash value –is produced that identifies the unique contents of the file. If the contents are modified in any way, the value of the hash will also change significantly.

signatures list (or hash codes list) of CAM that has already been vetted and accepted by law enforcement specialists as meeting the Baseline criteria. To be included in the IBH, material must meet the following criteria:

(1) It is already registered in the INTERPOL Child Sexual Exploitation database;

(2) The victim is a real child and prepubescent;

(3) The material depicts a sex act or is concentrated on the anal or genital region of the child;

(4) It is accepted as qualifying for IBH by three independent specialized officers from member countries connected to the International Child Sexual Exploitation Database and confirmed by expert staff at the General Secretariat.

17. On September 20, 2019, HSI Boston obtained a search warrant in the District of Massachusetts (Case Number 19-MJ-6412-MPK) to view the media file containing the image distributed by kidzklub and provided with the Kik report. On September 21, 2019, I reviewed the image and observed that it depicts a male between the ages of 11-12, posed standing fully nude, with his genitals exposed. Behind the minor victim, a male appearing to be an adult is posed standing fully nude, with both hands placed on the thighs of the minor victim. The erect penis of the adult male is visible between the legs of the minor victim.

18. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 24.61.82.255 was used by kidzklub on April 18, 2019 at 14:15:28 UTC to send the child pornography image. In addition, IP address

24.61.82.255 was used to access the Kik user account on more than 30 separate occasions during the same month the Kik user sent the child pornography image.

19. A query of the ARIN online database revealed that IP address 24.61.82.255 used on April 18, 2019 at 14:15:28 UTC to send a child pornography image was registered to Comcast.

20. On September 6, 2019, an administrative summons was issued to Comcast regarding the IP address during the specific date and time described in Paragraph 18. A review of the results obtained on September 9, 2019 identified the following account holder and address, which is the address of the SUBJECT PREMISES: Jim Lister, 74 Lancaster Road, Arlington, MA 02476.

21. When Kik discovers that an account is used to commit a child pornography offense, it bans the account. I am aware that the kidzklub account was closed by Kik when the known image of child pornography was transmitted on April 18, 2019.

KIK REPORT 3

22. I have reviewed a Kik report dated July 24, 2019. A review of the Kik Report shows that on July 24, 2019 an individual utilizing Kik username smudgedgraphite, who provided the name SmudgedGraphite**,** email address smudgedgrahite@gmail.com, and device brand and model Samsung SM-T580, used Kik to send an image of child pornography, as described herein.

23. I have learned that the Kik report for user smudgedgraphite was also triggered by utilizing SafePhoto technology and flagged based on a hash match with the INTERPOL database, as

described in Paragraph 16. The image which triggered the report was included within a media file and provided with the Kik report.

24. On February 6, 2020, HSI Boston obtained a search warrant in the District of Massachusetts to view the content contained in the media file provided with the Kik report for smudgedgraphite (Case Number 20-MJ-6032-MPK). On February 7, 2020, I reviewed the media image. The image depicts a boy between the ages of 9-11, nude from the waist down, posed bending forward over a bed. The boy's exposed genitals appear to be the focal point of the image.

25. The Kik report provided for smudgedgraphite provided IP addresses used by the account user to access the account. Specifically, IP address 24.34.109.218 was used by smudgedgraphite on July 24, 2019 at 21:55:03 UTC to send the child pornography image.

26. A query of the ARIN online database revealed that IP address 24.34.109.218 used on July 24, 2019 at 21:55:03 UTC to send a child pornography image was registered to Comcast.

27. On December 20, 2019, HSI Boston issued a summons to Comcast for the subscriber information regarding the IP address on the specific date time described in Paragraph 25. The following subscriber information was provided, which is the address of the SUBJECT PREMISES: Jim Lister, 74 Lancaster Road, Arlington, MA 02476.

28. When Kik discovers that an account is used to commit a child pornography offense, it bans the account. I am aware that the smudgedgraphite account was closed by Kik when the known image of child pornography was transmitted on July 24, 2019.

NEXUS TO THE SUBJECT PREMISES

29. Online property records for the SUBJECT PREMISES revealed the residence to be a single-family home, owned by James Lister. Queries of CLEAR[11], a law enforcement database, revealed residents of the address to be Mason LISTER (YOB 1995), James Lister, and Maureen Lister.

30. In September 2019, HSI Boston agents conducted open source checks of LISTER. There were several local news articles mentioning LISTER's 2016 and 2017 child pornography arrests in Massachusetts, due to LISTER trading child pornography on social media sites. LISTER was identified as a former daycare maintenance worker in Newton, Massachusetts, in a 2016 CBS Boston news article.

31. HSI Boston conducted a query of the Massachusetts Criminal Justice Information Services ("CJIS"), for Driver's Licenses associated with 74 Lancaster Road, Arlington, Massachusetts (the SUBJECT PREMISES). Results from CJIS identified Mason LISTER, James Lister, and Maureen Lister as holding valid Massachusetts Driver's Licenses at the SUBJECT PREMISES.

[11] CLEAR is a law enforcement database which maintains credit bureau information regarding address history, court records, property records, and vehicle information for individuals.

32. HSI Boston conducted criminal record checks of the residents of the SUBJECT PREMISES, with negative results for Maureen Lister and James Lister. A criminal history was located for Mason LISTER. LISTER was charged and convicted of the following offenses in the State of Massachusetts:

- 09/2016- Charged with Possession of Child Pornography and Distribution of Child Pornography in violation of Massachusetts General Laws (MGL) Chapter 272, Sections 29A and 29B and convicted on 3/29/2017.
- 07/2017- Charged with Possession of Child Pornography- 2 Counts, Subsequent Offense, and Distribution of Child Pornography, in violation of MGL Chapter 272, Sections 29A and 29B, and convicted 3/26/2018.

33. In October 2019, I contacted APD Detective Smith to advise him of the additional Kik leads involving the SUBJECT PREMISES. Smith confirmed the SUBJECT PREMISES to be the current address of LISTER.

34. Records I obtained from the Massachusetts Sex Offender Registry in July 2020 showed LISTER to maintain his current address as 74 Lancaster Road, Arlington, Massachusetts (the SUBJECT PREMISES). Massachusetts Sex Offender Registry documents also revealed that LISTER remains on probation with the State of Massachusetts for the offenses described in Paragraph 32 until March 26, 2022.

35. The Massachusetts Sex Offender Registry maintains LISTER's place of employment as the Shell Gas Station at 511 Totten Pond Road, Waltham, Massachusetts. On October 17, 2019, I

conducted surveillance at the location, and observed a Silver Toyota Camry, bearing Massachusetts registration 5VB852, parked behind the gas station convenience store at the address. I also observed LISTER inside the convenience store serving customers at the cash register.

36. On July 10, 2020, at approximately 9:45 a.m., I observed the same vehicle as described in Paragraph 35 in the driveway of the SUBJECT PREMISES, as well as a Maroon Toyota 4Runner bearing Massachusetts registration 196TZ3. RMV checks revealed the Toyota Camry to be registered to James Lister at the SUBJECT PREMISES, and the Toyota 4Runner to be registered to Maureen Lister at the SUBJECT PREMISES.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

37. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the

computer, using a cable or via wireless connections such as "WiFi[12]" or "Bluetooth[13]." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual

---

[12] WiFi is an abbreviation for wireless fidelity, which is a networking technology allowing computers, smartphones, and other devices to connect to the internet or communicate with one another wirelessly within a particular area.

[13] Bluetooth is a wireless technology standard used for exchanging data between fixed and mobile devices utilizing short-wavelength radio waves.

to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to

interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

38. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, possess, and/or access with intent to view child pornography.

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual

media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their pictures, films, video tapes, photographs, magazines, negatives, correspondence, mailing lists, books, tape recordings and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been

found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[14]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

---

[14] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

h. Even if a subject uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of Internet access will be found in a subject's home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

39. Based on the following, I believe that the user of gayinvaderzim and smudgedgraphite residing at the SUBJECT PREMISES likely displays characteristics common to individuals who distribute, possess, and access with intent to view child pornography. For example, an individual utilizing an IP address which resolved to the SUBJECT PREMISES sent two images of child pornography via the Kik app, once on April 18, 2019, from the kidzklub account, and again on July 24, 2019 from the smudgedgraphite account. As detailed herein, this individual utilizing internet access from the SUBJECT PREMISES distributed child pornography via Kik. In order to distribute such materials, the Kik user would necessarily have to acquire and possess child pornography.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

40. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic

storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

41. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application

operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

42. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the

dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under

investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a

dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

43. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or

destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

44. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems,

and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

45. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

46. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the location described in Attachment A. I respectfully request that this Court issue a search warrant for the location described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

47. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Sworn to under the pains and penalties of perjury,

/s/ Nicole Sorrell
_____
Nicole Sorrell
Special Agent
Homeland Security Investigations

SUBSCRIBED and SWORN before me telephonically pursuant to Fed. R. Crim. P. 41(d)(3) this 22 day of July, 2020.

_____
HONORABLE M. PAGE KELLEY
CHIEF UNITED STATES MAGISTRATE JUDGE

I have reviewed the images referenced in Paragraphs 17 and 24 above and I find probable cause to believe that they depict minors engaged in sexually explicit conduct. The affiant shall preserve the image provided to the Court for the duration of the pendency of this matter, including any relevant appeal process.

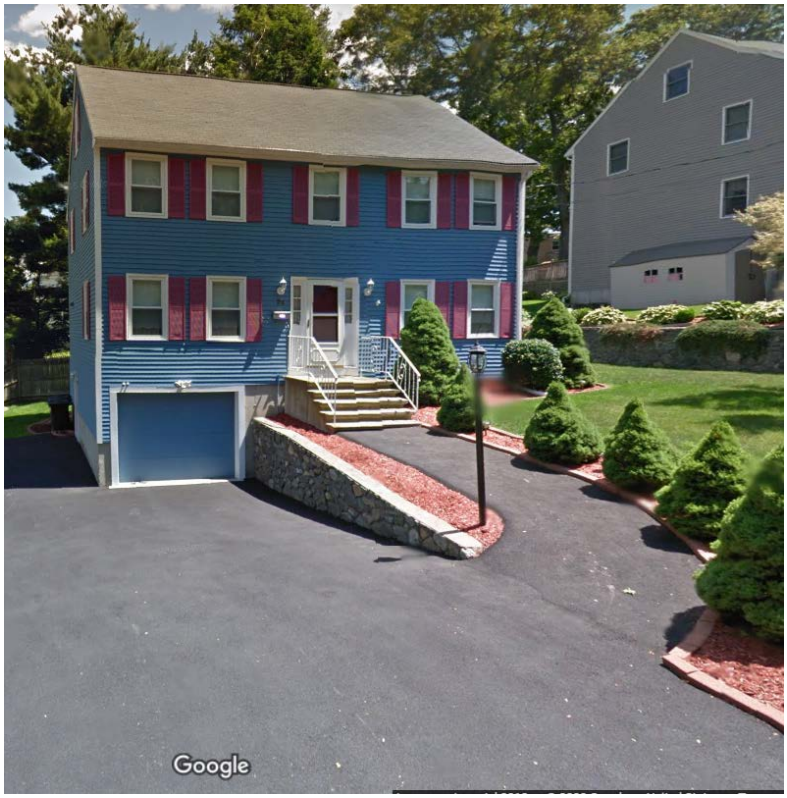
HONORABLE M. PAGE KELLEY
CHIEF UNITED STATES MAGISTRATE JUDGE

July 22, 2020

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The entire property located at 74 Lancaster Road, Arlington, MA 02476, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES), described as a blue, 2.5 story single-family home with the numerals "74" affixed to the left of the front door, as depicted below:



ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 2252A, including:

A. Records and tangible objects pertaining to the following topics:

1. Child pornography and child erotica; and

2. Communications with any other person that relates to the sexual exploitation of children.

B. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter forensic programs and associated data that are designed to eliminate data;

5. evidence indicating how and when the computer was accessed or used to

determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media;

8. documentation and manuals that may be necessary to access the computer equipment or to conduct a forensic examination of the computer equipment;

9. records of or information about Internet Protocol addresses used by the computer equipment;

10. records of or information about the computer equipment's Internet activity; and

11. contextual information necessary to understand the evidence described in this attachment.

C. Records, information, and items relating to the ownership or use of computer equipment and other electronic storage devices found in or on the LOCATION TO BE SEARCHED.

II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in Paragraph I.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

H. "Child Pornography," as defined in 18 U.S.C. § 2256(8)(A), means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

I. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.

EXECUTION

Searching agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence authorized by this warrant, as outlined above. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If the computer contains contraband, it will not be returned. If the computer equipment cannot be returned, agents will attempt to make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband or the fruits or instrumentalities of crime.